



**TRICARE Management Activity**  
**Protected Health Information Management Tool**  
**(PHIMT)**

**User Guide**  
**v1.0**

**Prepared By:**  
**Booz Allen Hamilton**

## Table of Contents

1.	GENERAL OVERVIEW .....	1
1.1	RESPONSIBILITIES AT THE MILITARY TREATMENT FACILITY (MTF) LEVEL .....	1
2.	GETTING STARTED .....	1
2.1	USER DEFINITIONS AND ROLES .....	1
2.2	ROLE/ORGANIZATION HIERARCHY .....	2
2.3	NOTICES AND TERMS OF USE .....	3
2.4	LOGGING IN .....	3
3.	GETTING FAMILIAR WITH PHIMT .....	4
3.1	PATIENT TAB .....	5
3.2	USER TAB .....	6
3.3	ADMIN TAB .....	6
3.4	REQUESTS TAB .....	7
3.5	REQUESTER TAB .....	8
4.	UPDATING USER PROFILE .....	8
4.1	SWITCHING ORGANIZATIONS .....	9
5.	PATIENT SEARCH/ ADDING A PATIENT .....	9
5.1	SEARCHING FOR A PATIENT .....	9
5.2	ADDING A NEW PATIENT .....	10
5.3	ADDING A PHONE NUMBER .....	11
5.4	ADDING AN ALTERNATIVE ADDRESS .....	11
6.	AUTHORIZATIONS .....	12
6.1	RECORDING AN AUTHORIZATION .....	12
6.2	ACCESSING/PRINTING THE AUTHORIZATION .....	14
6.3	REVOKING AN AUTHORIZATION .....	14
7.	RECORDING DISCLOSURES .....	15
7.1	DISCLOSURE REQUESTS .....	16
7.2	DISCLOSURE HYPERLINK .....	18
8.	AMENDING DISCLOSURES .....	18
9.	RESTRICTION OF DISCLOSURES .....	19
10.	SUSPENSION OF A DISCLOSURE .....	21
11.	ACCOUNTING FOR DISCLOSURES .....	22
11.1	REGULAR USER .....	22
11.2	PRIVACY SPECIALIST .....	24
12.	ADDITIONAL RESOURCES .....	26

## **1. GENERAL OVERVIEW**

The Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 require a covered entity, (i.e., the Military Health System (MHS)) to maintain a history of when and to whom disclosures of Protected Health Information (PHI) are made for purposes other than treatment, payment and healthcare operations (TPO). The MHS must be able to provide an accounting of those disclosures to an individual upon request. Authorizations and Restrictions from an individual to a covered entity are included in the information that is required for tracking purposes.

To comply with the requirements for disclosures, the TRICARE Management Activity (TMA) is providing an electronic disclosure-tracking tool. The Protected Health Information Management Tool (PHIMT) stores information about all disclosures, authorizations and restrictions that are made for a particular patient. PHIMT has a functionality built into it that can provide an accounting of disclosures, if necessary.

### **1.1 Responsibilities at the Military Treatment Facility (MTF) Level**

The MTF should have knowledge of DoD 6025.18-R, Health Information Privacy Regulation. A MTF must provide an accounting of disclosures within 60 days of the request. If the covered entity cannot honor an accounting of disclosures within the 60-day period, it must provide information to the requestor as to the reason for the delay and expected completion date. The covered entity may extend the time to provide the accounting by no more than 30 days. Only one extension is permitted per request.

## **2. GETTING STARTED**

The HIPAA Support Center creates an account for the User Admin and provides them with their User Name and Password. The User Admin is responsible for establishing all the accounts for their MTF. For more information on establishing accounts for MTFs, please refer to the PHIMT User Admin Manual.

### **2.1 User Definitions and Roles**

Each **User** is assigned to one or more organizations (an organization is a logical or physical entity such as an MTF, a Service or TMA).

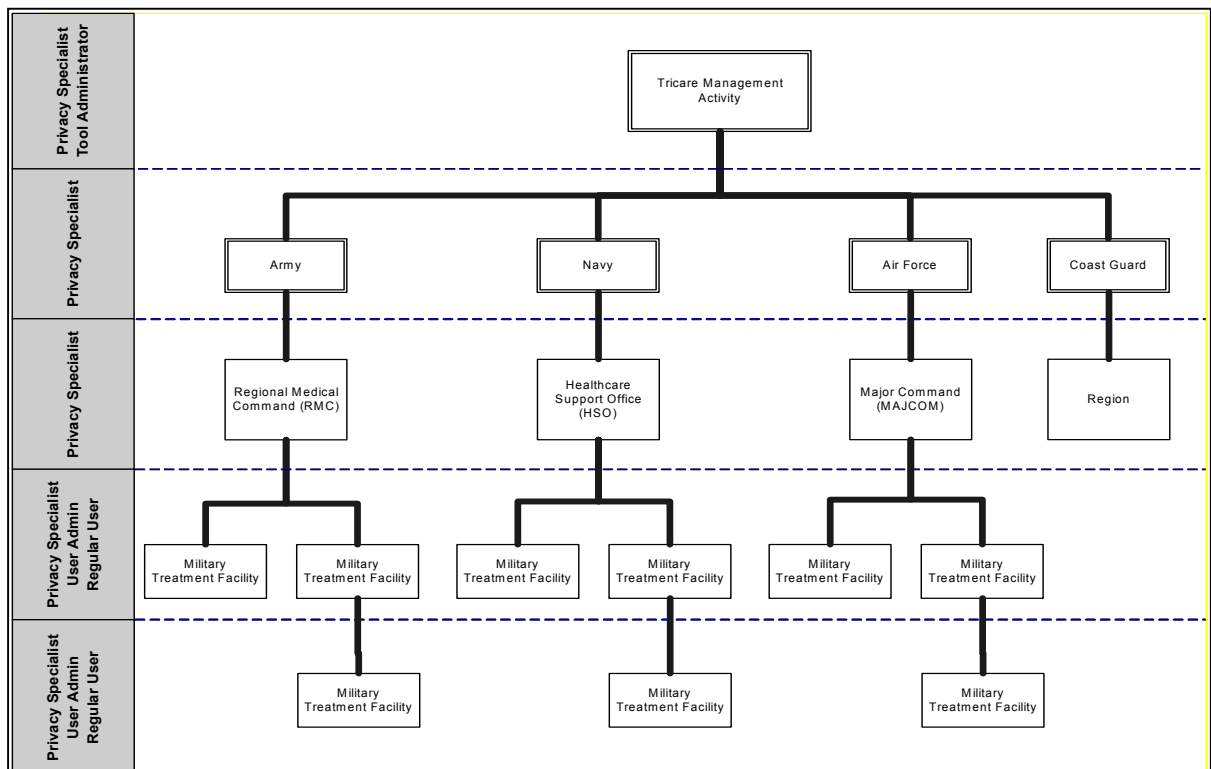
- Within an organization, each user can have one or more roles.
- A user can have the same roles in multiple organizations, or different roles in multiple organizations.
- Roles are inherited down the hierarchy.

A **Role** is a named collection of permissions. Roles allow Users with the same permissions to be grouped under a unique name. Examples of roles include: Regular User, User Admin, Privacy Specialist, and Tool Admin.

- A **Regular User** is a general role with basic functionality. This role can create disclosures and authorization requests that can be routed on to a Privacy Specialist.
- A **User Admin** is a local administrator for an MTF or a designated Service. This role allows one to add/modify users from within their Service and assigns roles. The email account administrators will handle this role for each MTF or Service.
- A **Privacy Specialist** is the Privacy Officer or designee at an MTF or Service level. This role allows the User to maintain disclosure reporting, approve/deny disclosure requests, amend requests, restrict and suspend disclosures, and to generate associated letters.
- A **Tool Administrator** has global access to the application and will be maintained by the HIPAA Support Center. This role allows the User to configure roles within MTFs, and create permissions within the application.

## 2.2 Role/Organization Hierarchy

The picture below illustrates the relationships of Users and Roles



## 2.3 Notices and Terms of Use

To login to PHIMT you must read and accept the Notices and Terms of Use when you access the URL. Then click Accept to move to the Login page.



**TRICARE**

**MHS Protected Health Information Management Tool**

THIS IS A DOD COMPUTER SYSTEM. THIS COMPUTER SYSTEM, WHICH INCLUDES ALL RELATED EQUIPMENT, NETWORKS, AND NETWORK DEVICES (SPECIFICALLY INCLUDING ACCESS TO THE INTERNET), ARE PROVIDED ONLY FOR OFFICIAL U.S. GOVERNMENT BUSINESS. DOD COMPUTER SYSTEMS MAY BE MONITORED BY AUTHORIZED PERSONNEL TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES. MONITORING INCLUDES "HACKER" ATTACKS TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM AGAINST USE BY UNAUTHORIZED PERSONS. DURING THESE ACTIVITIES, INFORMATION STORED ON THIS SYSTEM MAY BE EXAMINED, COPIED AND USED FOR AUTHORIZED PURPOSES AND DATA OR PROGRAMS MAY BE PLACED INTO THIS SYSTEM. THEREFORE, INFORMATION YOU PLACE ON THIS SYSTEM IS NOT PRIVATE. USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO OFFICIAL MONITORING OF THIS SYSTEM. UNAUTHORIZED USE OF A DOD COMPUTER SYSTEM MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE PROVIDED TO APPROPRIATE PERSONNEL FOR ADMINISTRATIVE, CRIMINAL, OR OTHER ACTION.

**PRIVACY ACT WARNING**

INFORMATION CONTAINED IN THIS SYSTEM IS SUBJECT TO THE PRIVACY ACT OF 1974 (5 U.S.C. 552A, AS AMENDED). PERSONAL INFORMATION CONTAINED IN THIS SYSTEM MAY BE USED ONLY BY AUTHORIZED PERSONS IN THE CONDUCT OF OFFICIAL BUSINESS. ANY INDIVIDUAL RESPONSIBLE FOR UNAUTHORIZED DISCLOSURE OR MISUSE OF PERSONAL INFORMATION MAY BE SUBJECT TO FINE OF UP TO \$5,000.

Accept

## 2.4 Logging In

1. Login using the User Name and Password that has been assigned to you by your User Admin. If you have not received your User Name or Password or you need to have your password reset, contact your User Admin.



**TRICARE**

**MHS Protected Health Information Management Tool**

Information entered into this version will not be retained.  
This is for training and testing purposes only.

User Name:

Password:

Login

Enter the same User Name and Password as you use when signing on to the MHS network

2. The first time you login you will be prompted to change the temporary password assigned by the User Admin. The password must be 6 to 15 characters long and contain at least one:
  - Alphabetic uppercase character
  - Alphabetical lower case character
  - Arabic numeral (0,1,2,3,4)
  - Non-alphanumeric special character (i.e.,!,@,#,\$, etc)

**Change Password**

**Error(s) have occurred:**  
 ■ This is a temporary password, please change it now.

---

**Old Password** (Password that you are currently using.)

**New Password** (New password you want to use.)

**Confirm New Password** (Confirm your new password.)

---

Copyright © HIPAA Accelerator, Inc. 2000-2003, ALL RIGHTS RESERVED

### 3. GETTING FAMILIAR WITH PHIMT

Your assigned role (i.e. Privacy Specialist) determines the level of access and permissions within the tool. The complete PHIMT screen contains five tabs, each with their own functionality:

- Patient Tab
- User Tab
- Admin Tab
- Requests Tab
- Requestor Tab

Depending on an individual's role within the tool, not all tabs will be available.

Wednesday, October 1, 2003 Patient Search Help Logout

Patient User Admin Requests Requester

**Current User:**  
Chris Foster  
US TMA

My Profile  
My Requests  
My Worklist

[Switch organizations](#)

**User Worklist**

Activity	Request	Activity ID	Source	Patient	Requester	Status	Creation Date
Instance ID	Session ID						

---

Copyright © HIPAA Accelerator, Inc. 2000-2003, ALL RIGHTS RESERVED

### 3.1 Patient Tab

The **Patient** tab provides access to information by a specific patient name. To access database records a user must first select a patient.

The Patient Summary screen will display the following viewing options: Disclosures, Suspensions, Restrictions, Reports, Letters, Authorizations, Notices and Complaints. In the Summary Items Filter box a user can select the appropriate checkboxes to view individually or can select the **All** checkbox to view all associated records.

Monday, October 6, 2003 Patient Search Logout

Patient User Admin Requests Requester

**Current Patient:**  
Mark Sean Thomas  
1001/1905  
FMP-SSSN 01-  
123456789

**Patient Summary**

Summary Item Filters Display

☐ All ☐ Disclosures ☐ Suspensions ☐ Restrictions ☐ Reports ☐ Letters ☐ Authorizations ☐ Notices ☐ Complaints

Summary  
Requests  
Record Disclosure  
Accounting Suspensions  
Disclosure Restrictions  
Authorization  
Notice  
Patient Profile  
Relationships  
Patient Search

Copyright © HIPAA Accelerator, Inc. 2000-2003. ALL RIGHTS RESERVED

Based on a user's role, a user may access the following activities from the left side of the screen on the Patient tab by clicking on any of these hyperlinks:

- Summary - shows a summary of all entries for a particular patient.
- Record Disclosure - allows Privacy Specialists to enter a disclosure of PHI.
- Accounting Suspensions - allows users to enter an accounting suspension for a patient.
- Disclosure Restrictions - allows a user to place restrictions on who receives a patient's PHI.
- Authorization - allows a user to enter an authorization for releasing PHI.
- Patient Profile - allows the user to look at the patient profile they are working with.
- Patient Search - allows the user to search for any patient in the database.

Wednesday, October 1, 2003 Patient Search Help Logout

Patient User Admin Requests Requester

**Current Patient:**  
None

**Patient Search**

Name (First, Last)

System ID (the identifier created by this system for the person)

External ID (an external identifier for the person)

Search

Copyright © HIPAA Accelerator, Inc. 2000-2003. ALL RIGHTS RESERVED

### 3.2 User Tab

The **User** tab contains all PHIMT User related information. The User tab is designed to track all tasks that are assigned to you. The User Worklist serves as your electronic inbox. It is advised that you review your User Worklist to verify the any tasks that has been assigned to you.

Based on your role PHIMT users will have the following access in the User Tab by clicking on the hyperlinks:

- My Profile - where users update their information and create user-to-user relationships.
- My Requests - where users can see status of all requests that they initiated.
- My Worklist - where users can see and process all requests that have a task currently assigned to them for work.
- Switch Organizations - where users that are assigned to more than one organization can switch between their organizations.

### 3.3 Admin Tab

Based on your role the **Admin** tab is used to regulate administrative functions of the database including maintaining disclosure types, manual retrievers, and organizations; and also creating/modifying users. The Tool Admin role will maintain the Disclosure Type Management, Codes Management, Authorization Type Management and Permission Management hyperlinks.

*Note: If there is a request for a new type of administrative function, please contact the HIPAA Support Center.*



- Disclosure Type Management - allows the Admin to create Disclosure Types and specify their details.
- Invoice Defaults Management - allows the setup of the system invoicing functionality
- Codes Management - allows for the setup of system reference data. Reference data appears in the drop down lists throughout the system.
- Authorization Type Management - allows for authorization types (types of authorizations) to be created and edited.
- PHI Source Management - allows the Admin to create and/or modify PHI Source details for the PHIMT Database.
- Organizational Management - allows the Admin to create and/or modify organizations within the PHIMT Database.
- Permission Management - allows for the setup of permissions. Also allows the Admin to assign different system permissions to user roles. Permission could provide access to a screen or function.
- All Users List - allows for user management.
- User Search
- Add User

### 3.4 Requests Tab

Based on your role you will have access to the following request options:

- Complaint
- Disclosure
- Disclosure Accounting

By selecting a Request option and pressing the **Next** button a user will be guided through a step-by-step process for completing an action.

The screenshot shows a web application interface. At the top, there is a header bar with the date 'Monday, October 6, 2003' on the left and 'Patient Search' and 'Logout' links on the right. Below the header is a navigation menu with tabs for 'Patient', 'User', 'Admin', 'Requests', and 'Requester'. The 'Requests' tab is currently selected. The main content area is titled 'Create New Request'. On the left side of this area, there is a sidebar with the text 'Current Request: None' and two links: 'Create New Request' and 'Search for a Request'. The main part of the form is titled 'Select Request Type' and contains three radio button options: 'Disclosure Accounting', 'Complaint', and 'Disclosure'. The 'Disclosure' option is selected, indicated by a filled radio button.

- Complaint - A lodged complaint can be entered into the system and tracked as needed.
- Disclosure - A request for a disclosure can be entered into the system and routed as needed.
- Disclosure Accounting - A request for an Accounting of Disclosures can be entered into the system and routed as needed.
- Create New Request - The default page for entering a new request.
- Search for a Request - Search for a request that has been placed within your organization.

### 3.5 Requester Tab

Based on your role the Requester tab provides access to all PHIMT Requester data.

The screenshot shows the 'Requester Search' interface. At the top, there's a navigation bar with tabs: Patient, User, Admin, Requests, and Requester. The 'Requester' tab is selected. On the left, a sidebar shows 'Current Requester: None' and links for 'Requester Summary', 'Requester Requests', and 'Requester Profile'. The main area is titled 'Requester Search' and contains three search options: 'Select a Third-Party Organization', 'Search for a Person', and 'Search for an Organization'. Each option has input fields and a 'Search' button. There are also checkboxes for 'Include Patient Records' and 'Include Non-Patient Records'. A footer note states: '\* You must search for an existing requester or requesting organization before adding a new one.' The copyright notice at the bottom reads: 'Copyright © HIPAA Accelerator, Inc. 2000-2003, ALL RIGHTS RESERVED'.

- The Requester Summary Screen contains the option to display letters generated for requesters.
- Requester Requests - a hyperlink where users can see status of all requests associated with a select requester.
- Requester Profile - a hyperlink where users can see and update the requester's demographic information.

## 4. UPDATING USER PROFILE

Please contact your User Admin to update to your profile. PHIMT contains profiles for all users within the system. It is important to keep this information up to date; therefore all personal information should be updated as it changes. The following process is used to update your User Profile in the PHIMT.

1. Click on **User** tab
2. Click on **My Profile** hyperlink located on the left side of the screen.

The screenshot shows the 'User Profile' interface. At the top, there's a navigation bar with tabs: Patient, User, Admin, Requests, and Requester. The 'User' tab is selected. On the left, a sidebar shows 'Current User: Chris Foster, US TMA' and links for 'My Profile', 'My Requests', and 'My Worklist'. The main area is titled 'User Profile' and contains fields for 'Name', 'Phone', 'System ID', 'User ID', 'Email', 'Password Locked', 'Old Password', 'New Password', and 'Confirm New Password'. There is also a 'Comments' field at the bottom. The footer note states: '\* You must search for an existing requester or requesting organization before adding a new one.' The copyright notice at the bottom reads: 'Copyright © HIPAA Accelerator, Inc. 2000-2003, ALL RIGHTS RESERVED'.

2. Verify information is correct. *Note: Please remember that a phone number will display on letters when generated.*
3. Enter correct information as needed.
4. Click **Update** button.

#### 4.1 Switching Organizations

Users that are assigned to more than one organization have the ability to switch their organization from the User tab.

1. Select **User** tab.
2. Click on the **Switch Organization** hyperlink.

ID	Name	Address
26	82 Airborne	
24	89th MED GRP-ANDREWS [DMIS 0066]	89 Medical Group, 1050 West Perimeter RD, Andrews AFB, MD 20762-6600
19	Army DEA	123 Maple St, Fairfax, VA 12345
48	Carefirst BCBS	7 Commerce Dr., P.O. Box 1685, Cumberland, MD 21502
17	DEA	123rd, Burkw, Burke, VA 22015
18	DEA Army	4565 Main St, Main, VA 10000
38	FBI	567 Main St, Washington, DC 12345
37	FBI Megan	123 Main St, Burke, VA 22015
25	FT MEADE - KIMBROUGH ACC [DMIS 0069]	Kimrough Ambulatory Care Cent, 2480 Llewellyn Ave., Ft. Meade, MD 20755-5900
29	Ft Myer Aid Station	
28	Ft Myer Aid Station	
45	HSI	1052 State St., Kirtland Afb, NM 23456
44	HSI	
30	James Brown	
40	MID	666 Sunnydale Dr, Pleasantville, IL 13131
23	NDC GREAT LAKES [DMIS 0494]	NDC GREAT LAKES [DMIS 0494], Bldg 73, Great Lakes, IL 60088-5258

3. Select the organization that you need to switch to.
4. Click **Select**.
5. Under Current User in the top left corner you will see the organization you have switched to.

## 5. PATIENT SEARCH/ ADDING A PATIENT

### 5.1 Searching for a Patient

The search feature in PHIMT allows you to find a patient that has already been added to the system. To search for a patient please follow the steps below:

1. Click on **Patient** tab.

## 2. Click on **Patient Search**

3. Enter a patient's last name **or** the first several letters of the patient's last name followed by an asterisk within the Patient Last Name field.
4. Click **Search**.
5. If the search returns no matches then there are two possible reasons:
  - a. Your search criteria are not correct.
  - b. The patient record does not exist.

## 5.2 Adding a New Patient

When adding a new Patient record, conduct a search within the system initially to ensure that it does not already exist. Patient records must be added to the system before disclosures, authorizations or restrictions can be documented.

1. Click on **Patient** tab.
2. Search for Patient.  
*Note: Refer to Searching for a Patient*
3. If patient is not listed on results, click the **Create a New Patient Record** hyperlink located on the bottom of the screen.

4. Fill in the required fields: First Name, Last Name, and Birth Date in MM/DD/YYYY format, Type, SSN, and FMP-SSSN for the member. Click the **Save** button.
5. Fill in the required fields: Address, City, State, and the Zip Code. In the Timezone field, enter the appropriate time zone. Click the **Save** button.

### 5.3 Adding a Phone Number

1. Select the **Patient Profile** hyperlink.
2. To add a phone number, scroll down to the Associated Addresses box. Click on the ID of the address that needs the phone number added.
3. Scroll down to the Associated Phones box. Click the **New** button.
4. Enter a phone number (Area code in first box, ###-#### in second box, and Extension if necessary in third box). Click the **Save** button.
5. Click the **Update** button within the address screen.
6. The Patient Profile Screen will display indicating you have completed this task.

### 5.4 Adding an Alternative Address

Based on your role you could be responsible for entering and processing the Request for Alternate Communication Address. A Patient can request that all communication containing PHI be sent to an address different from their home address.

1. Click on **Patient** Tab.
2. Click on **Patient Search**.
3. Enter a patient's last name **or** the first several letters of the patient's last name followed by an asterisk within the Patient Last Name field.
4. Click **Search**.
5. If the search returns no matches then there are two possible reasons:
  - a. Your search criteria are not correct.
  - b. The patient record does not exist.
6. Click on the **Patient Profile** hyperlink located on left side of screen.

7. Scroll to the bottom of the Patient Profile screen; click the **Alternate Communication** button in the Associated Addresses box.

Comments (general comments about or for the person)

Update

Associated Addresses		New	Alternate Communication			
ID	Street	City	State	Zip	Alternate	Primary
10	105 Chestnut St	Chicago	IL	60600	No	<input checked="" type="radio"/>

Copyright © HIPAA Accelerator, Inc. 2000-2003, ALL RIGHTS RESERVED

8. Fill in the required fields: Address, City, State, and the Zip Code. In the Timezone field, select the appropriate time zone.
9. In Outcome field, make selection from drop down list:
- Selecting *Approved* records the address as an Alternate Communication Address. This action will record the address in PHIMT as Primary and will generate an approval letter to be sent to the alternate address.
  - Selecting *Denied* records the request for an Alternate Communication Address. This action will record the address in PHIMT as active but the address is not listed as Primary and it generates a denial letter to be sent to the Primary address.
10. Click the **Save** button.

## 6. AUTHORIZATIONS

### 6.1 Recording an Authorization

The following process is used to record an Authorization by the patient when there is an exchange of PHI that occurs outside of TPO.

1. Click on **Patient** tab.
2. Click on **Patient Search**.
3. Enter a patient's last name **or** the first several letters of the patient's last name followed by an asterisk within the Patient Last Name field.
4. Click on **Search**.
5. If the search returns no matches then there are two possible reasons:
  - a. Your search criteria are not correct.
  - b. The patient record does not exist.

6. Click on the **Authorization** hyperlink located on the left side of the screen

7. Select an authorization type from the **Type** drop down list.  
*Note: Based on the Type Selected, the following fields are populated; however that data can be changed.*
8. Enter the Protected Health Information to be released as it was entered on the authorization form.  
*Note: The greater specificity that is provided by the patient, the easier it will be to respond to the request at the time of disclosure.*
9. Enter the Reason for Request/Use of Medical Information by selecting the appropriate checkbox or entering data in the Other field.
10. Enter the Recipient information
11. Enter the Authorization Start Date using (MM/DD/YYYY) format or use the calendar icon to select a date.
12. You must also enter either Authorization Expiration or an Action Completed. If there is no expiration date then text should be entered in the Action Completed field (i.e. Authorization to remain in effect until revoked).
13. Generate an authorization by selecting the checkbox for Generate Authorization.
14. Click **Save**.

*Note: Once the authorization has been manually signed one can go back into the particular authorization and select the **Signed** checkbox and enter the date of the signature using (MM/DD/YYYY) format or use the calendar icon to select a date.*

## 6.2 Accessing/Printing the Authorization

Once the Authorization has been recorded, the following process is used to access/print the authorization.

1. Click on the **Summary** hyperlink.

Friday, October 24, 2003 Patient Search Logout

Patient User Admin Requests Requester

**Current Patient:**  
Frank Thomas  
09/29/2003  
RWP-SSSN12-3456789

**Patient Summary**  
An alternate address exists for this patient.

**Summary Item Filters** Display

☐ All ☐ Disclosures ☐ Suspensions ☐ Restrictions ☐ Reports ☐ Letters ☒ Authorizations ☐ Notices ☐ Complaints

**Authorizations (Revoked authorizations are highlighted in red)**

ID	Title	Description	Signed	Expiration	Revoked
65	Psychotherapy Notes	For disclosures of 'medical records' to 'Frank Thomas'		10/24/2004	
64	Psychotherapy Notes	For disclosures of 'medical records' to 'Frank Thomas'		10/24/2004	
63	Psychotherapy Notes	For disclosures of 'medical records' to 'John Smith 1234 something Ave Something, VA 23987'	10/23/2003	10/23/2004	
60	Psychotherapy Notes	For disclosures of 'complete medical record' to 'John Smith something something'	10/23/2003		10/23/2003

Copyright © HIPAA Accelerator, Inc. 2000-2003. ALL RIGHTS RESERVED

2. Select Authorizations by putting a check mark in the correct box.
3. Click **Display**.
4. Select the correct Authorization title to generate the Authorization form.
5. Print the form for the patient's signature.

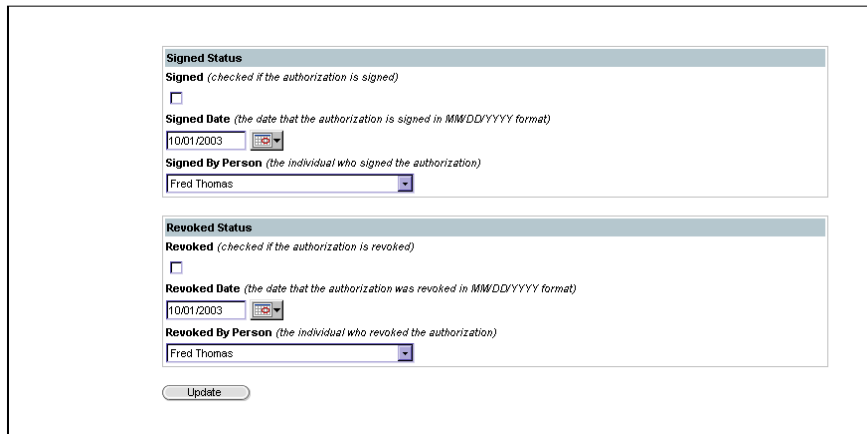
## 6.3 Revoking an Authorization

The following process is used to revoke an Authorization. The patient may revoke an Authorization by requesting it in writing.

1. Click on the **Patient** tab.
2. Click on **Patient Search**.
3. Enter a patient's last name **or** the first several letters of the patient's last name followed by an asterisk within the Patient Last Name field.
4. Click **Search**.
5. If the search returns no matches then there are two possible reasons:
  - a. Your search criteria are not correct.
  - b. The patient record does not exist.
6. Select **Authorizations** from the Summary Items Descriptions and click **Display**.



7. Select the associated ID Number of the specific authorization that is being revoked. The Patient Authorization Management screen will display.
8. Scroll to the bottom of the Patient Authorization Management screen and mark the **Revoked** checkbox.



The screenshot displays a web form for managing patient authorizations. It is divided into two main sections: 'Signed Status' and 'Revoked Status'. The 'Signed Status' section includes a checkbox for 'Signed (checked if the authorization is signed)', a date field for 'Signed Date (the date that the authorization is signed in MM/DD/YYYY format)' with a calendar icon, and a dropdown menu for 'Signed By Person (the individual who signed the authorization)' currently showing 'Fred Thomas'. The 'Revoked Status' section includes a checkbox for 'Revoked (checked if the authorization is revoked)', a date field for 'Revoked Date (the date that the authorization was revoked in MM/DD/YYYY format)' with a calendar icon, and a dropdown menu for 'Revoked By Person (the individual who revoked the authorization)' also showing 'Fred Thomas'. At the bottom of the form is an 'Update' button.

9. Enter the date of the revocation, using MM/DD/YYYY format or use the calendar icon to select the date.
10. Enter the name of the Patient or the Patient's legal representative who is revoking this Authorization in the Revoked by Person field.
11. Click the **Update** button.

## 7. RECORDING DISCLOSURES

Depending on your role within PHIMT, disclosures can be recorded two ways:

- Disclosure Requests
- Disclosure Hyperlink

The Disclosure Requests is available to Regular Users and Privacy Specialist. Privacy Specialists can also use the Disclosure hyperlink to record disclosures. Privacy Specialists who are recording disclosures for approval should use the hyperlink. Using the Disclosure Requests, a disclosure can only be forwarded on for approval/denial.

## 7.1 Disclosure Requests

The Disclosure Requests can be used by Regular Users to forward disclosures to the Privacy Specialist for approval or denial.

1. Click on the **Requests** tab.

Monday, October 6, 2003 Patient Search Logoff

Patient User Admin **Requests** Requester

**Current Request:** None

**Create New Request**

☐ Create New Request  
☐ Search for a Request

**Select Request Type**

☐ Disclosure Accounting  
☐ Complaint  
☒ Disclosure

2. Select the Disclosure by clicking on the small circle radio button and click **Next**.
3. Enter a patient's last name **or** the first several letters of the patient's last name followed by an asterisk within the Patient Last Name field.
4. Click **Search**.
5. If the search returns no matches then there are two possible reasons:
  - a. Your search criteria are not correct.
  - b. The patient record does not exist
6. Select **OK** button.
7. Select the Requester.

Monday, October 6, 2003 Patient Search Logoff

Patient User Admin **Requests** Requester

**Current Request:** Disclosure

☐ Create New Request  
☐ Search for a Request

**Requester Search**

Choose one of the following options:

**Select the Patient** (the request is being made by the patient themselves)

Mark Sean Thomas Select

**Select a Third-Party Organization** (a third-party requester, such as a law enforcement agency or insurance company)

Army FBI, 9024 Rosewall Ct., Columbus, OH 22212 Select

**Search for a Person** (search for another person, or add a new one\*)

**Name** (First, Last, An "\*" may be used as a wildcard.)

**System ID** (the identification number created by this system for the person)

**External ID** (an external identifier for the person)

☒ Include Patient Records  
☒ Include Non-Patient Records

Search

**Search for an Organization** (search for another organization, or add a new one\*)

**Name** (All or part of the name of the organization. An "\*" may be used as a wildcard.)

Search

\* You must search for an existing requester or requesting organization before adding a new one.

8. Confirm the Requester and Recipient Details, click **Next**.

Monday, October 6, 2003 Patient Search Logout

Patient User Admin Requests Requester

Current Request: Disclosure

Select Patient Select Requester Request Details Disclosure Details Request Action

1 2 3 4 5

■ Create New Request  
■ Search for a Request

### Confirm Requester and Recipient Details

**Patient:** Mark Sean Thomas  
**Date of Birth:** 1985-10-01  
**SSN:** 000000000  
**Address:** 231 Fish Ln., Cod, MD 20000

**Requester:** Mark Sean Thomas [change](#)  
**Address:** 231 Fish Ln., Cod, MD 20000 [Add New](#)

**Recipient:** Same as requester  
[set a different recipient](#)

[Back](#) [Next](#)

9. Enter the Request details, click **Next**.

Patient User Admin Requests Requester

Current Request: Disclosure

Select Patient Select Requester Request Details Disclosure Details Request Action

1 2 3 4 5

■ Create New Request  
■ Search for a Request

### Request Details

**Details of the Request** (requester's comments, or instructions about this request)

**Requester Identity Verified** (was the requester's identity verified?)  
 Undefined

**Description of Requester Identity Verification** (if the requester's identity was verified, how was it verified?)

**Requester Authority Verified** (was the requester's authority to access information verified?)  
 Undefined

**Description of Requester Authority Verification** (if the requester's authority was verified, how was it verified?)

**Information Start Date** (the start date for the information in MM/DD/YYYY format)

**Information End Date** (the end date for the information in MM/DD/YYYY format)

**Request Format** (the format in which this request has been received)  
 Undefined

10. Enter Disclosure Details, click **Next**.  
*Note: Disclosure status will be set to Pending because Regular Users do not have the authority to approve Disclosures.*
11. Enter the Action Requested from the **Action** drop down menu.
- Privacy Specialist – can route to own worklist for approval/denial or route to another Privacy Specialist
  - Regular User – Can route to own worklist for further research or route to a Privacy Specialist
12. Click on **Save** to process the Disclosure Request.

## 7.2 Disclosure Hyperlink

The second method to record disclosures is through accessing the Record Disclosure hyperlink. The Disclosure hyperlink is located on the left of the Patient Tab screen but is only available to specific roles.

1. Click on **Patient Search**.
2. Enter a patient's last name **or** the first several letters of the patient's last name followed by an asterisk within the Patient Last Name field
3. Click **Search**.
4. If the search returns no matches then there are two possible reasons:
  - a. Your search criteria are not correct.
  - b. The patient record does not exist
5. Select the **Record Disclosure** hyperlink located on the left side of the screen.

6. Complete all fields in the Patient Disclosure form.  
*Note: You have the ability to complete the Disclosure in the Disclosure Status field*
7. Select **Save** when you have completed all fields pertaining to the disclosure.  
*Note: The Disclosure Type and Disclosure Purpose cannot be set to Undefined.*

## 8. AMENDING DISCLOSURES

Once a Disclosure has a Disclosure Status of completed, the only way to amend it is by assigning it as an Improper Disclosure. In the event that a disclosure must be labeled as an Improper Disclosure the Privacy Specialist must:

1. Click on **Patient** Tab.

2. Click on **Patient Search**.
3. Enter a patient's last name **or** the first several letters of the patient's last name followed by an asterisk within the Patient Last Name field.
4. Click **Search**.
5. If the search returns no matches then there are two possible reasons:
  - a. Your search criteria are not correct.
  - b. The patient record does not exist
6. In the Patient Summary Screen select Disclosures, and then click **Display**.
7. Select the Improper Disclosure by clicking on the associated **ID** in the Disclosures box.
8. Scroll to the bottom of the Patient Disclosure screen and locate the Improper Disclosure section.

The screenshot shows a web form for managing patient disclosures. At the top, there are several checkboxes for selecting the type of disclosure: History and Physical Examination, Laboratory Test(s), Operative Report(s), Pathology Report(s), and Progress Notes. Below these is an 'Other:' field with a text input and a dropdown arrow. The 'Disclosure Comments' section includes a text input with the placeholder 'send to home address' and a dropdown arrow. The 'Improper Disclosure' section features a checkbox labeled 'Improper Disclosure (checked if this disclosure occurred improperly)'. Below this is the 'Improper Disclosure Description' section with a text input and a dropdown arrow. The 'Improper Disclosure Mitigation' section also has a text input and a dropdown arrow. At the bottom of the form is an 'Update' button.

9. Select the **Improper Disclosure** checkbox.
10. Fill out the Improper Disclosure Description.
11. Fill out the Improper Disclosure Mitigation.
12. Click **Update**.
13. Re-create the disclosure, if necessary, with the correct information.

## 9. RESTRICTION OF DISCLOSURES

Regular Users and Privacy Specialists are able to enter a Restriction of Disclosure or terminate a Restriction of Disclosure. Restriction of Disclosures allows members to restrict uses and disclosure of their PHI.

1. Click on **Patient** Tab.
2. Click on **Patient Search**.
3. Enter a patient's last name **or** the first several letters of the patient's last name followed by an asterisk within the Patient Last Name field.
4. Click **Search**.
5. If the search returns no matches then there are two possible reasons:
  - a. Your search criteria are not correct.
  - b. The patient record does not exist
6. Click within the radio button to select the specific member. Click **Select**.
7. Click on the **Disclosure Restrictions** hyperlink located on the left side of the screen.
8. On the Patient Disclosure Restriction History Screen, click **New**.
9. Select the Disclosure Type field and make a selection.  
*Note: If a new Disclosure Type is needed please contact the HIPAA Support Center.*

The screenshot shows a web application interface for 'Patient Disclosure Restriction'. At the top, there's a navigation bar with tabs: Patient, User, Admin, Requests, and Requester. Below this, a sidebar on the left lists various functions: Summary, Requests, Record Disclosure, Accounting Suspensions, Disclosure Restrictions, Authorization, Notice, Patient Profile, Relationships, and Generate Form. The main content area is titled 'Patient Disclosure Restriction' and contains several form fields:
 

- Current Patient:** Mark Smith Thomas, 1001/1995, FMP-SSSN 01-123456789.
- Disclosure Type:** A dropdown menu with 'Medical Facility Patient Directories' selected.
- Start Date:** A text field with a calendar icon, labeled '(The start date from which US TMA will not share this information with identified party, in MM/DD/YYYY format)'.
- End Date:** A text field with a calendar icon, labeled '(The OPTIONAL end date at which time US TMA will begin to share this information again, in MM/DD/YYYY format)'.
- Restriction Destination:** A text field labeled '(to whom information is being restricted?)'.
- Details of Restriction:** A large text area labeled '(what information is being restricted?)'.
- Outcome:** A dropdown menu with 'Approved' selected, labeled '(indicate whether request was approved or denied)'.
- A 'Save' button at the bottom.

10. Enter a start date using MM/DD/YYYY or the calendar icon in the Start Date field.
11. If an end date is available for the request, enter it in the End Date field.
12. In the Restriction Destination field enter to whom the information is being restricted from.
13. Enter the specific details of what information is being restricted.  
*Note: It is important to be specific in this entry because this will provide other staff members with the details about the individual and organization, and about the restrictions on the disclosure.*

14. In the Outcome field, select Approve or Deny from the drop down list. A corresponding approval or denial letter will be generated.
15. Click the **Save** button.
16. Scroll down the Patient Disclosure Restriction screen and locate the Letters box. Click on the link for the appropriate letter and view it in PDF format.

## 10. SUSPENSION OF A DISCLOSURE

A Suspension of Disclosure occurs when an agency requests that the MTF not include a disclosure made during the course of an investigation to a patient when they request their Accounting of Disclosures. The following two types can be suspended: Law Enforcement Purposes and Health Oversight Activities.

1. Click on the **Patient** tab.
2. Click on **Patient Search**.
3. Enter a patient's last name **or** the first several letters of the patient's last name followed by an asterisk within the Patient Last Name field.
4. Click **Search**.
5. If the search returns no matches then there are two possible reasons:
  - a. Your search criteria are not correct.
  - b. The patient record does not exist.
6. Click within the radio button to select the specific member, and then click the **Select** button.
7. Select the **Accounting Suspensions** hyperlink located on the left side of the screen.

Wednesday, October 1, 2003 [Patient Search](#) [Help](#) [Logout](#)

Patient User Admin Requests Requester

**Current Patient:**  
Mark Sean Thomas  
10/01/1985  
FMP-SSSN:01-  
123456789

Summary  
Requests  
Record Disclosure  
Accounting Suspensions  
Disclosure Restrictions  
Authorization  
Notice  
Patient Profile  
Relationships  
Generate Form

[Patient Search](#)

### Patient Disclosure Suspension History

Disclosure Accounting Suspensions					
Suspension ID	Suspended Disclosure	Identifier	Start Date	End Date	Comments

**Create New Disclosure Accounting Suspension**

For the current Patient, suspend their disclosure accounting rights for a **specific disclosure**. Use this to suspend a single disclosure.

For the current Patient, suspend their disclosure accounting rights for a **type of disclosure**. Use this to suspend more than one disclosure of a particular type.

Copyright © HIPAA Accelerator, Inc. 2000-2003, ALL RIGHTS RESERVED

8. The Patient Disclosure Suspension History screen will display. From here you will have two options to create a Suspension:
  - a. Specific Disclosure - creates a suspension for one particular disclosure.
  - b. Type of Disclosure - creates a suspension for all disclosures of a particular type.
9. Select which type of suspension is needed from the New Disclosure Accounting Suspension box.
10. Complete all necessary fields.
11. Click the **Save** button.

## 11. ACCOUNTING FOR DISCLOSURES

A Patient may ask for an Accounting of Disclosure at any time. The PHIMT allows for a quick Accounting of Disclosures. The steps to follow for creating an Accounting of Disclosures will depend on whether you are a Regular User or a Privacy Specialist.

### 11.1 Regular User

1. Click the **Requests** tab.
2. Click on **Disclosure Accounting**.
3. Enter a patient's last name **or** the first several letters of the patient's last name followed by an asterisk within the Patient Last Name field.
4. Click **Search**.
5. If the search returns no matches then there are two possible reasons:
  - a. Your search criteria are not correct.
  - b. The patient record does not exist
6. If the Requester is the same as Patient, then click the **Select** button below Requester's name.
7. Choose the appropriate Requester and click the **Search** button.
8. Click within the radio button to select the specific requester. Click the **Select** button.



9. If the Requester is not found, either the name you are searching for is not spelled correctly or there is not a Requester by that name in the database. In this case you will need to enter a new Requestor into the database.

10. Confirm Requestor and Recipient Details and click the **Next** button.
11. Complete the details of the Request Field.
12. If the Requester's identity has been verified, select the Requester Identity Verified drop down menu and choose a value.
13. Enter the Report Start Date and Report End Date fields.
14. Make a selection from the Request Format drop down menu.
15. Make a selection from the Request Clarification drop down menu and select **Next**.
16. Complete the necessary fields in the Request Action screen, and click **Save**.  
*Note: You can route to your Privacy Specialist for approval or denial or to your own worklist if you need to do further research.*

## 11.2 Privacy Specialist

To account for disclosures a Privacy Specialist must:

1. Click the **Requests** Tab.
2. Click on **Disclosure Accounting**.
3. Enter a patient's last name **or** the first several letters of the patient's last name followed by an asterisk within the Patient Last Name field.
4. Click **Search**.
5. If the search returns no matches then there are two possible reasons:
  - a. Your search criteria are not correct.
  - b. The patient record does not exist.
6. If the Requester is the same as Patient, click the **Select** button below Requester's name.
7. Choose the appropriate Requester and click the **Search** button.
8. Click within the radio button to select the specific requester. Click the **Select** button.
9. If the Requester is not found, either the name you are searching for is not spelled correctly or there is not a Requester by that name in the database. In this case you will need to enter a new Requestor into the database.

**Requester Search**

Choose one of the following options:

**Select the Patient** (the request is being made by the patient themselves)

Mark Sean Thomas

**Select a Third Party Organization** (a third-party requester, such as a law enforcement agency or insurance company)

Army FBI, 9024 Roosevelt Ct., Columbus, OH 22212

**Search for a Person** (search for another person, or add a new one\*)

Name (First, Last. An "\*" may be used as a wildcard.)

System ID (the identification number created by this system for the person)

External ID (an external identifier for the person)

☒ Include Patient Records

☒ Include Non-Patient Records

**Search for an Organization** (search for another organization, or add a new one\*)

Name (All or part of the name of the organization. An "\*" may be used as a wildcard.)

\* You must search for an existing requester or requesting organization before adding a new one.

10. Confirm Requestor and Recipient Details and click the **Next** button.
11. Complete the Details of the Request Field.

12. If the Requester's identity has been verified, select the Requester Identity Verified drop down menu and choose a value.
13. Enter the Report Start Date and Report End Date fields.
14. Make a selection from the Request Format drop down menu.
15. Make a selection from the Request Clarification drop down menu and select **Next**.
16. Complete the necessary fields in the Request Action screen.

Wednesday, October 1, 2003 Patient Search Help Logout

Patient User Admin Requests Requester

Current Request: Disclosure Accounting

Select Patient Select Requester Request Details Request Action

1 2 3 4

Create New Request  
Search for a Request

**Request Action**

**Patient**  
Name: Mark Thomas  
SSN #: 000000000  
Birth Date: 10-01-1985  
Address: 231 Fish Ln., Cod, MD 20000

**Requester/Recipient**  
Name: Mark Sean Thomas  
Address: 231 Fish Ln., Cod, MD 20000

**Details of the Request** (requester's comments about the scope of this request)

**Approved Part** (for partially approved requests, describe part of request that was approved)

**Denied Part** (for partially denied requests, describe part of request that was denied)

**Action** (choose one of the following actions for this request)  
Route to Privacy Specialist

Back Save

- Route To My Worklist - allows a Privacy Specialist to place it in their worklist to follow up on when appropriate.
- Process Request Now - allows a Privacy Specialist to place it in their worklist for approval.
- Deny Request Now - allows a Privacy Specialist to deny the disclosure.
- Route to Privacy Specialist - allows a Privacy Specialist to pass the disclosure on to another Privacy Specialist to be processed, as established in a User-to-User Relationship.
- Route to Other User - allows a Privacy Specialist to pass the disclosure back to another user to process the letter generation after approving/denying the request, as established in a User-to-User Relationship.

17. Click **Save**.

## 12. ADDITIONAL RESOURCES

- DoD 6025.18-R, “DoD Health Information Privacy Regulation”, January 2003
- **[www.tricare.osd.mil/hipaa](http://www.tricare.osd.mil/hipaa)** TMA HIPAA Website
- **[hipaamail@tma.osd.mil](mailto:hipaamail@tma.osd.mil)** for subject matter questions
- **[hipaasupport@tma.osd.mil](mailto:hipaasupport@tma.osd.mil)** for tool related questions
- Your Service HIPAA representatives